Encryption Policy
January 2000
Questions and Answers

General Policy

1. Why is the Administration revising its encryption export policy?
The Vice President promised that we would continue to review our encryption policy and make the necessary updates to adjust it to the global market for information technology while protecting the needs of privacy, national security and law enforcement. On September 16, 1999, the U.S. announced a new approach to its encryption control policy. The core of the export part of this policy rests on three principles: a technical review of encryption products in advance of sale, a streamlined post-export reporting system that takes into account industry's distribution models, and review of some exports to foreign government end-users.

2. What is the encryption update based on?
In September, we announced a new paradigm that is essential to protect America's prosperity and security and is comprised of three elements: information security and privacy, a new framework for export controls and updated tools for law enforcement. The new approach recognizes that encryption is a vital component of the emerging global information infrastructure and digital economy.

Classification

3. Do I have to submit source code for a review and classification of my encryption product?
For certain products, government review of source code may be required as provided in Supplement 6 to part 742. As with all transactions, the U.S. government considers this information confidential. Please note that publicly available source eligible under sections 740.13(e) and 740.17(a)(5)(i) does not require prior review and classification but rather written notification by the time of export.

4. What happens to the pending license applications and classification requests that were submitted before the regulation was published?
The new regulation contains a "grandfathering" clause that allows exporters to use License Exception ENC to non-government end-users if their encryption commodity or software was previously reviewed under a license, Encryption Licensing Arrangement or received License Exception ENC eligibility. Most of the pending applications will be approved with a clarifying statement that the products are now eligible for License Exception ENC. However, to determine if your product qualifies for "retail", a separate classification and review is required by BXA. Additionally, pending applications will be reviewed under the new policy.

5. When does the 30 day clock start for classification requests?
The 30 day clock begins on the day BXA receives your classification request, and it is logged into our system. You should check the automated system "STELA" by calling 202-482-2752. Your application must be in the system for 30 calendar days before you can use the provision to export to non-government end-users under License Exception ENC, unless otherwise notified by BXA.

6. If after 30 days I do not hear from BXA, and I export my encryption product, will it delay or influence my "retail" classification request?
No, your classification request will not be delayed or treated any differently than any other application.

7. How do I track the process of my classification request?
You may call "STELA" to determine if your classification request is entered into our system at 202-482-2752. If you do not hear from us, your request is moving through the review process. Please read the relevant parts of the Export Administration Regulation (EAR) to determine where your product fits within the encryption policy and Supplement 6 to Part 742 of the (EAR) before you submit your classification request. Also, additional guidance is located on the webpage for submitting both license applications and classification requests. If we have any questions or need more information, we will contact you.

8. Where do I send classification requests, key length increase certification letters and post-export reports?
(A) For classification requests, send the **original** BXA Form 748P, 748P-A (if applicable) and support documents to the Bureau of Export Administration, U.S. Department of Commerce, 14th Street and Pennsylvania Avenue, N.W., Room 2705, Washington, D.C. 20444, Attn: "Application Enclosed". A **copy** of the entire application (forms and supporting documents) must also be mailed to Attn: ENC Encryption Request Coordinator, 9800 Savage Road, Suite 6131, Ft. Meade, MD 20755-6000.

(B) For post-export reports and certification letters, you may submit them electronically to **crypt@bxa.doc.gov** (suggested file formats include spreadsheets, tabular text or structured text), or to the Department of Commerce, Bureau of Export Administration, Office of Strategic Trade and Foreign Policy Controls, 14th Street and Pennsylvania Avenue, N.W., Room 2705, Washington, DC 20230, Attn: Encryption Reports. A copy must also be mailed to Attn: ENC Encryption Request Coordinator, 9800 Savage Road, Suite 6131, Ft. Meade, MD 20755-6000.

9. Is there a review of the foreign product developed with U.S. encryption?
No, a review of the foreign product is not required, unless the encryption item was exported to a U.S. subsidiary. The developed encryption product requires a review and classification, since the original export to the U.S. subsidiary was not reviewed by BXA.

10. Are all encryption items excluded from the de minimis provision?
Certain encryption items controlled under ECCNs 5A992, 5D992 and 5E992 may be eligible for de minimis after review and release from "EI" controls. These items include 56-bit encryption commodities, software and technology with asymmetric key exchanges not exceeding 512-bits, 512-bit key management products and 64-bit mass market encryption commodities and software.

Internet Posting and Sales

11. For Internet exports, what constitutes reasonable and sufficient screening procedures to implement any restrictions that do exist under the regulations on exports to foreign government end-users?
The website must be configured to check the Internet Protocol (IP) address of the person requesting the encryption product for transfer or download to ensure that the requester's address is not a foreign government domain name. In addition, the receiver of the encryption download or transfer must indicate that the software is not intended to be used by a government end-user. The website must also inform the receiver or requestor the software is subject to the EAR, and it cannot be transferred without a license or other authorization. See Section 734.2(b)(9)(iii).

12. Does posting encryption source or object code on the Internet constitute an export under the EAR?
Yes, it can as the definition of the export of encryption source code and object code software under the provisions of section 734.2(b)(9) includes such action. For publicly available source code under sections 740.13(e) and 740.17(a)(5)(i), while such source code is exempted under section 734.2(b)(9)(ii) and (iii), and is thus not subject to those provisions (including screening procedures), the source code nonetheless remains subject to the EAR. Please note that section 734.2(b)(9)(i) defines "export" to include the actual shipment, transfer, or transmission out of the United States or transfer in the United States to an embassy or affiliate of a foreign country. For all other encryption source code and object code software, posting constitutes an export unless the person making the software available on the Internet takes precautions to prevent unauthorized transfers.

13. Does the mere posting of publicly available source code establish knowledge of any prohibited export or reexport?
Posting of publicly available source code on the Internet (e.g., FTP or World Wide Web site), where it may be downloaded by anyone, would not establish "knowledge" (as that term is defined in the EAR) of a prohibited export or reexport, i.e., an export or reexport that would otherwise require a license. Such posting would not trigger "red flags" necessitating the affirmative duty to inquire under the "Know Your Customer" guidance provided in Supplement No. 3 to Part 732. Compliance with EAR requirements as to prohibited exports and reexports (see the General Prohibitions in Part 736) still apply. So, for example, a license would be required for you to e-mail or directly transfer such source code to a national located in a prohibited country (e.g, Sudan) or to a prohibited end-user (e.g., an entity listed on BXA's Entity List found at

Supplement No. 4 to Part 744).

14. Would posting to a "newsgroup" site fall within the types of eligible Internet posting methods for publicly available source code eligible under Section 740.13(e), License Exception TSU?
Yes. The listing of eligible Internet postings described in License Exception TSU, e.g., FTP and World Wide Web site, is illustrative in nature, not exclusive.

15. Can an academic who creates an encryption source code program make it available on the Internet, for example to students or academic colleagues, without restriction on access?
Yes, under the revised regulations, encryption source code that would be publicly available (and posting to the Internet itself would make it publicly available), and which is not subject to an express agreement for the payment of a licensing fee or royalty for the commercial production or sale of any product developed using the source code, would be eligible under License Exception TSU for "unrestricted" source code. Under this policy, the software may be exported without prior submission to the government for technical review (although concurrent notification of the export is required). In addition, software exported under this exception may be posted to the Internet without restriction and would not be subject to any requirement to screen for access. Also, such posting would not constitute knowledge of an export to a prohibited destination under the EAR, including one of the seven terrorist states. A license requirement would apply only to knowing exports and reexports (i.e., direct transfer or e-mail) of the software to prohibited end-users and destinations. In addition, exporters are not restrained from providing technical assistance (as described in Section 744.9) to foreign persons working with such source code.

16. Will an intellectual property protection, such as a copyright, by itself, be construed as an express agreement for the payment of a licensing fee or royalty for the commercial production or sale of any product developed using the source code that would make encryption source code not eligible for export under License Exception TSU for publicly available "unrestricted" source code?
No.

17. Am I required under the EAR to actively screen for terrorist-supporting destinations?
In your business practice, it is prudent to use a standard of care to ensure that you will not violate any of the prohibition identified in the EAR. The EAR does not require a person posting software on the Internet to implement screening procedures for the terrorist countries. For publicly available source code exported under a license exception, once such source code is posted to the Internet, a license requirement exists or remains for "knowing" transfers (i.e., direct transfer or e-mail) to a prohibited end-user or destination. For any "retail" or other encryption software exported under a license exception by means of Internet posting, export restrictions to the seven terrorist states remain in place and exporters should take the steps necessary to prevent an export in violation of such restrictions. The "Know Your Customer" guidance in Supplement No. 3 to Part 732 provides companies with guidelines on how to comply with their

responsibilities under the EAR. Please note that section 734.2(b)(9)(iii) contains screening procedures to prevent the transfer of certain encryption software to foreign government end-users.

"Retail" Products

18. How will the "retail" section of License Exception ENC be implemented?

A classification is necessary to determine whether an encryption product qualifies as "retail". The review process will be similar to what has been done in the past, however, exporters should review the retail section of License Exception ENC and address how their products meet the listed criteria. BXA will work with exporters to gather any additional necessary information. We intend that this review and classification will take no longer than other classification requests.

19. Can you elaborate on the criteria used for defining "retail" products? Is it based on the distribution model and not the strength of the encryption?

Criteria:

The "retail" section of License Exception ENC contains four categories of encryption products.

The first set is encryption commodities or software that are generally available to the public by being (1) sold through retail outlets, (2) specially designed for individual consumer use, **or** (3) sold in large volume without restrictions through mail order, electronic or telephone sales. For encryption products to qualify as "retail" under this first part, your encryption product has to be distributed in one of these three ways. However, these products must not:

(a) allow the cryptographic functionality to be easily changed by the user, (b) does not require substantial support to install and use, (c) is not modified or customized for the customer and (d) is not designed to be used as network infrastructure products. If your product meets the above criteria, then it may be considered "retail". The regulation contains an illustrative but not restricted list of examples of the types of products that are considered "retail" under this section. All of this is taken into account to qualify for "retail", it is not based on the key length of the encryption items.

The second category of encryption products are those that function similarly to other products classified as "retail". The products are reviewed for their overall functionality and not simply its security functions. We intend to compare products which are similar in function, but may be incorporated differently, i.e., bundled vs. standalone.

The third category of products are finance-specific products that are restricted by design for such functions as e-commerce and financial transactions. These products are highly field formatted and are not capable of performing general purpose encryption, such as e-mail messaging. Inclusion in this category is not based on the algorithm keysize.

The fourth category are non-mass market 56-bit products with asymmetric key exchanges between 512 to 1024-bits. These products are based on the key length of the encryption.

20. What "amount" is required for a product to qualify as "sold in large volume"?
A "retail" encryption product that is "sold in large volume" is produced and widely available through various distribution methods. While there is not an exact amount, most products that will qualify under this set are produced in the thousands of units per month. It is understood that it most likely take time for a start-up company to establish its products in the marketplace. However, it should be made clear that newly released beta products may not qualify in this category.

21. What is the difference between the definitions of "retail" and "mass market"?
We recognize that certain encryption products are distributed through various channels, making it impossible, in practical terms, to control who the end-user may be. We have accommodated several of industry's aims by creating a new regulatory category called "retail". While the "retail" and the category "mass market", which is used in the Wassenaar Arrangement, are not equivalent, the retail definition includes significant flexibility. In practice, we expect many classifications as retail.

22. What is meant by the term "equivalent functionality" in the "retail" criteria?
The term "equivalent functionality" is not limited to comparing two products' encryption security features. Rather it is the overall functionality of the entire product. We intend to scrutinize and compare products that function similarly, regardless if the product contains embedded capabilities or is a standalone item.

23. Could you elaborate on what constitutes a low-end server, router or firewall in the "retail" criteria?
Our intent is to allow low-end servers, routers and firewalls that are designed for small office networks or home offices to qualify for "retail". Products are sold in large volume and widely available through various distribution methods. While there is not an exact amount, most products that will qualify under this set are produced in the thousands of units per month. These are encryption products that are not designed to handle large throughput or network traffic.

Telecommunications and Internet Service Providers

24. What type of services require a license?
In certain instances, a license is required to provide encryption services to government end-users. Under License Exception ENC, Internet and telecommunications service providers may use retail products to provide service to any end user. However, they will require a license to provide services using products not classified as retail to government end users. Examples are WANs, LANs, VPNs, voice and dedicated-link services; application specific and e-commerce services,

and PKI encryption services specifically for government end-users only.

25. When exports and reexports are made to Telecommunications and Internet Service Providers, I need to report on "network infrastructure" products that have not qualified as retail by the time of export. What are some examples of "network infrastructure" products?
Examples of "network infrastructure" products include high-end switches or routers, which are designed for larege volume communications.

Reporting Requirements

26. Do I have to report exports shipped before the date of the regulation to non-U.S. banks and financial institutions?
No, post-export reporting is effective the date the regulation was published.

27. How do I determine whether the export of my "retail" product is being purchased and used by an individual, or is being purchased and used by an individual for multiple commercial use?
When an individual buys a "retail" product, there is no reporting requirement. However, companies may determine this in a variety of ways, e.g., the number of seats or user licenses purchased, screening for business vs. individual uses, etc.

28. What do you mean by "if collected" in the reporting requirements?
During the normal course of business, exporters may gain information about the ultimate end-user depending on their contractual relationship with the distributor or reseller. In these instances, BXA would like that information included in their reports. This clause is not designed to alter or strain the exporter's current business practice.

Government End-Users

29. How do I determine if my customer is a "government end-user"?
The new regulation adds a definition of "government end-user" in Part 772. The definition covers government organizations at the central, regional, and local levels which are departments, agencies, or entities performing governmental functions. Review the definition carefully for examples of organizations that are included in the definition and organizations which are not. For example, a governmental corporation that manufactures or distributes items or services controlled on the Wassenaar Munitions List is a "government end-user." (You can access the Wassenaar Munitions List at the following URL address: www.wassenaar.org.)

Excluded from the definition are organizations that may be wholly or partially government-owned, but have certain specific purposes. Such organizations include utilities, such as gas, electricity, telecommunications providers and Internet service providers; transportation, such as train systems, subway systems and airport authorities, broadcast or entertainment, such as

television broadcasters; educational organizations, such as schools, colleges and universities; civil health and medical organizations, such as hospitals and clinics; retail or wholesale firms; and manufacturers or industrial entities that do not manufacture or distribute Wassenaar List items or services.

If you are unsure of whether a particular end user meets the definition, you may submit an advisory opinion request to the Bureau of Export Administration, or submit a license application for your transaction.

30. What is the licensing policy for exports of encryption products to government end-users?

The licensing policy for exports of encryption products to entities that meet the "government end-user" definition is described in Section 742.15(b)(3). Applications for civil end uses, such as social or financial services to the public, civil justice, social insurance pensions and retirement, taxes, and communications between governments and their citizens will be favorably considered. This reflects the existing licensing practice for government end users. Applications for other end uses will be reviewed on a case-by-case basis.

31. If a U.S. company and foreign government end-user both own a percentage of a foreign company, is that company considered a "government end-user"?

In such cases involving foreign government ownership, exporters must review the definition of "government end-user" to see if the foreign company qualifies. However, control or involvement of a foreign government in the foreign subsidiary of the U.S. company does not constitute ownership.

Licensing Policy

32. Can I submit an ELA for government end-users? How about for exports of technology?

In general, you will have to submit individual licenses for exports of encryption products to entities that meet the "government end-user" definition. However, applications for ELAs for government end users may be considered on a case-by-case basis. In such applications, you should be as specific as possible concerning the country or countries, the government entity or entities who will be using the products, and the end-use of the product.

Exporters may submit applications for ELAs for exports of encryption technology to strategic partners of U.S. companies. In addition, foreign companies with subsidiaries in the United States may apply for ELAs to export encryption technology to its worldwide locations. All ELA applications will be reviewed on a case-by-case basis.

33. What are the technical parameters for mass market products in the newly created Cryptography Note?

The Cryptography Note in Part 774 states that ECCNs 5A002 and 5D002 do not control encryption items that meet certain distribution and technical criteria. The technical criteria are that the cryptographic functionality cannot be easily changed by the user, the product is designed for installation by the user without further substantial support by the supplier, and the product does not contain a "symmetric algorithm" using a key length greater than 64-bit. Technical information on the product must be available, upon request, to BXA. Note that exporters are not permitted to self classify items that meet the criteria of the Cryptography Note, but must submit the product to BXA for review.

34. Is an open cryptographic interface the same as a "crypto-with-a-hole" product?
Yes. Any product that contains an interface that is not fixed and that permits a third party to insert cryptographic functionality, needs a binding mechanism to be considered a closed interface and eligible for License Exception ENC treatment. Exporters are encouraged to review the updated definition for "open cryptographic interface" in part 772.

35. May I use License Exception ENC to export encryption items to Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria?
You must apply for a license to export encryption items to the above-noted terrorist-supporting countries as well as other embargoed destinations, e.g., Serbia and the Taliban controlled areas of Afghanistan. For specific information, you may contact BXA's Office of Strategic Trade & Foreign Policy Controls or, depending on the country, the Treasury's Office of Foreign Asset Controls (URL: www.treas.gov/ofac).

36. Are all encryption items "grandfathered"?
Most encryption items are "grandfathered" if they were previously reviewed under a license, Encryption License Arrangement (ELA) or classified as eligible to use License Exception ENC. You may now use License Exception ENC to export to non-government end-users, except classifications under License Exception ENC granted to U.S. subsidiaries.

37. Are there export control restrictions on transfers of encryption items within the same country?
In-country transfers of encryption items (which have not been classified as retail) to foreign government end-users are prohibited unless otherwise authorized by license or license exception.

38. May I use License Exception ENC to export encryption technology to my foreign parent?
License Exception ENC, as it pertains to exports of technology (not products), can only be used if the end-user meets the definition of U.S. subsidiary (as defined in Part 772 of the EAR). Exporters may submit ELAs to export technology to their foreign parent or subsidiaries, however, the foreign product developed with this technology is not subject to a review and licensing by BXA.

39. Can I increase the key length of my product without another review?
You may increase the confidentiality or key exchange algorithm's key length of your encryption product without another review, e.g., 56-bit DES to 168-bit 3DES, and be eligible for export under License Exception ENC to any non-government end-user. However, no other change in the encryption functionality is permitted under this provision in the EAR. A letter certifying the key length increase should be sent to BXA.

40. Can you self-classify an encryption item?
All encryption items controlled under ECCNs 5A002, 5D002 and 5E002 require a review, either through a classification request or a license (both an individual license or an ELA), by BXA. (This review requirement does not apply to publicly available source code eligible under sections 740.13(e) and 740.17(b)(5)(i), which require written notification by the time of export.)

On the other hand, there are three types of products being decontrolled under this regulation that require a review before export: (1) 64-bit mass market commodities and software, (2) 56-bit commodities, software and technology with asymmetric algorithms of 512-bits and (3) 512-bit key management products. Once reviewed, they will be classified under ECCNs 5A992, 5D992 and 5E992.

Reminder: encryption commodities and software specified under *related controls* under ECCN 5A002 on the Commerce Control List (CCL) do not require review (i.e., access control systems, data authentication equipment, certain smart cards, certain cellular telephones, etc.); however, we do suggest that you have these items formally classified by BXA if you are unsure of the proper classification.

41. If I am sending encryption technology to a U.S. subsidiary under License Exception ENC, what are my obligations under this new policy?
You are not required to submit any documentation to BXA prior to export nor are there any reporting requirements; however, a review and classification will be required before any sale or transfer outside of the U.S. company.

42. If I want to export encryption commodities and software (in object code) that I know does not meet the "retail" definition, what are my obligations under this new policy?
You are required to submit a classification request to BXA prior to exporting to all non-government end-users and there are some post-export reporting requirements; however, there are no further licensing restrictions. Exporters should also review section 740.17(e)(2) regarding grandfathering of existing products, in which case an additional classification is not required.

43. If I want to export encryption components, toolkits and source code (other than to my U.S. subsidiaries) that's neither considered publicly available nor qualifying under the

"retail" definition, what are my obligations under this new policy?
You are required to submit a classification request to BXA prior to exporting to all non-government end-users and there are some post-export reporting requirements; however, there are no further licensing restrictions.

44. Can you expand on what my specific reporting obligations are when exporting encryption components, toolkits and source code that's not publicly available?
When sold to foreign manufacturers, post-export reporting is limited to the name and address of the manufacturer plus any non-proprietary information of the foreign products developed when manufactured for commercial sale. If for the manufacturer's internal use, only the name and address is required.

45. Is the Administration committed to reviewing and updating the encryption policy this year?
In developing this regulation, the Administration worked closely with stakeholders to assure a workable and balanced approach. Over the next 6 months, the Administration will review the workability of the regulation, and receive public comments for 120 days. A final revised rule will be issued shortly thereafter.

46. Will the U.S. update its encryption policy sooner if the European Union implements an EU license-free zone?
A number of companies have expressed concern that the European Union (EU) may implement a general authorization permitting encryption items to be exported freely within the EU and other specified countries. If and when the EU implements such an authorization, the Administration will take the necessary steps to ensure U.S. exporters are not disadvantaged.